PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-196084
(43)Date of publication of application : 21.07.1999

(51)Int.Cl. H04L 9/10
G06F 13/00
G06F 15/00
G11B 20/10
H04L 9/08

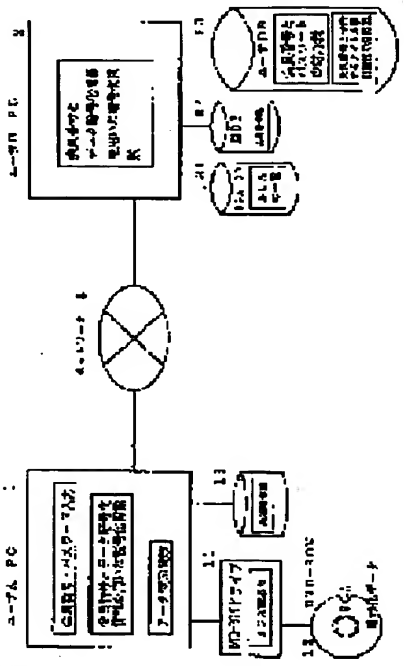
(21)Application number : 09-327170
(22)Date of filing : 13.11.1997

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : URANAKA SACHIKO
KIYONO MASAKI
TATEBAYASHI MAKOTO

(30)Priority
Priority number : 09314544 Priority date : 31.10.1997 Priority country : JP

(54) CIPHERING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To distribute a common cipher key used to decipher data of a ciphered DVD-ROM with a simple device and a simple procedure securely.
SOLUTION: A terminal 1 is provided with a DVD-ROM driver 11, a means that sends a key data request to a center device via a communication channel, and a means that decodes a ciphered common cipher key based on a combination of a part of burst cutting area(BCA) data and a membership number. A center device 2 is provided with a means that retrieves a user database 23, in response to a key data request to authenticate the user, a means that retrieves BCA data base 21 to obtain BCA data for the user, a means that obtains the common cipher key by retrieving a key database 22, and a means that ciphers the common cipher key, based on the combination of a part of burst cutting area BCA data and the membership number and transmits the resulting key. Since the combination of a part of burst cutting area BCA data already distributed and the membership number is used for a key to cipher the common cipher key, the common cipher key is ciphered securely with a simple device and a simple procedure, and the resulting key is transmitted.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－196084

(43)公開日　平成11年(1999)７月21日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｈ０４Ｌ	9/10		Ｈ０４Ｌ	9/00	６２１Ａ
Ｇ０６Ｆ	13/00	３５１	Ｇ０６Ｆ	13/00	３５１Ｚ
	15/00	３３０		15/00	３３０Ｇ
Ｇ１１Ｂ	20/10		Ｇ１１Ｂ	20/10	Ｈ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｅ

審査請求　未請求　請求項の数８　ＦＤ　（全 11 頁）　最終頁に続く

(21)出願番号　特願平9－327170

(22)出願日　平成９年(1997)11月13日

(31)優先権主張番号　特願平9－314544

(32)優先日　平９(1997)10月31日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　浦中　祥子
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　清野　正樹
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

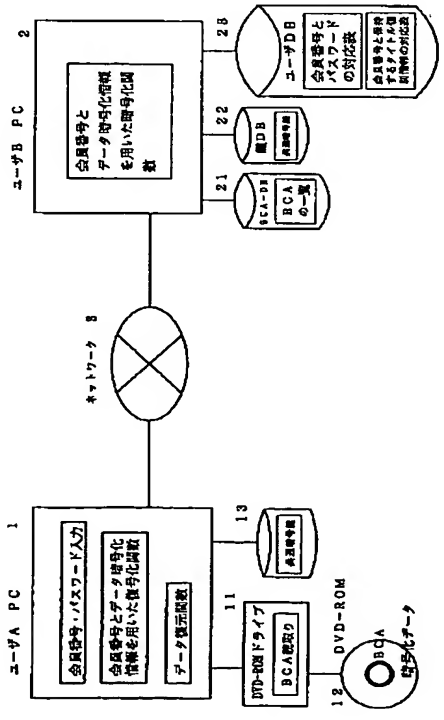
(74)代理人　弁理士　役　昌明　（外３名）

(54)【発明の名称】　暗号化システム

(57)【要約】

【課題】　暗号化ＤＶＤ－ＲＯＭのデータを解読する共通暗号鍵を簡単な装置と手順で安全に配布する。

【解決手段】　端末装置１に、ＤＶＤ－ＲＯＭドライブ11と、鍵データ要求を通信回線を介してセンター装置に送る手段と、暗号化された共通暗号鍵をＢＣＡデータの一部と会員番号を組み合わせたもので復号する手段を設ける。センター装置２に、鍵データ要求に応じてユーザデータベース23を検索してユーザを認証する手段と、ＢＣＡデータベース21を検索してユーザのＢＣＡデータを求める手段と、鍵データベース22を検索して共通暗号鍵を求める手段と、ＢＣＡデータの一部と会員番号を組み合わせたもので共通暗号鍵を暗号化して送信する手段とを設ける。既に配布済みのＢＣＡデータの一部と会員番号を組み合わせたものを、共通暗号鍵を暗号化する鍵とするので、簡単な装置と手順で安全に共通暗号鍵を暗号化して送ることができる。



【特許請求の範囲】

【請求項１】　データを暗号化するデータ暗号化装置と、その暗号化されたデータを解読する暗号データ解読装置とから構成され、それらの間ではネットワークやバス等を介してデータの送受信が可能であり、
前記暗号データ解読装置は、それぞれに固有な媒体固有情報を有する可搬性記憶媒体を駆動する手段と、データ要求を前記データ暗号化装置に送る手段と、前記データ暗号化装置から受信したデータを前記媒体固有情報で復号する手段とを備え、
前記データ暗号化装置は、可搬性記憶媒体それぞれに固有な媒体固有情報を蓄積するデータベースと、前記データベースを検索して前記データ要求に対応する媒体固有情報を求める手段と、要求されたデータを前記媒体固有情報で暗号化して送信する手段とを備えた、暗号化システム。

【請求項２】　データを暗号化するセンター装置と、その暗号化されたデータを解読する端末装置とから構成され、それらの間ではネットワークやバス等を介してデータの送受信が可能であり、
前記端末装置は、それぞれに固有な媒体固有情報であるＢＣＡデータを有するＤＶＤ－ＲＯＭを駆動する手段と、データ要求を前記センター装置に送る手段と、前記センター装置から受信したデータを前記ＢＣＡデータで復号する手段とを備え、
前記センター装置は、ＤＶＤ－ＲＯＭそれぞれに固有なＢＣＡデータを蓄積するＢＣＡデータベースと、前記データベースを検索して前記データ要求に対応するＢＣＡデータを求める手段と、要求されたデータを前記ＢＣＡデータで暗号化して送信する手段とを備えた、暗号化システム。

【請求項３】　データを暗号化するデータ暗号化装置と、その暗号化されたデータを解読する暗号データ解読装置とから構成され、それらの間ではネットワークやバス等を介してデータの送受信が可能であり、
前記暗号データ解読装置は、それぞれに固有な媒体固有情報を有する可搬性記憶媒体を駆動する手段と、データ要求を前記データ暗号化装置に送る手段と、前記データ暗号化装置から受信したデータを前記媒体固有情報で復号する手段とを備え、
前記データ暗号化装置は、可搬性記憶媒体それぞれに固有な媒体固有情報を蓄積する媒体固有情報データベースと、本システムを利用するユーザに関する情報を蓄積するユーザデータベースと、前記データ要求に応じて前記ユーザデータベースを検索して前記暗号データ解読装置のユーザを認証する手段と、前記媒体固有情報データベースを検索して前記データ要求に対応する媒体固有情報を求める手段と、要求されたデータを前記媒体固有情報で暗号化して送信する手段とを備えた、暗号化システム。

【請求項４】　データを暗号化するデータ暗号化装置と、その暗号化されたデータを解読する暗号データ解読装置とから構成され、それらの間ではネットワークやバス等を介してデータの送受信が可能であり、
前記暗号データ解読装置は、それぞれに固有な媒体固有情報を有する可搬性記憶媒体を駆動する手段と、鍵データ要求を前記データ暗号化装置に送る手段と、前記データ暗号化装置から受信した鍵データを前記媒体固有情報で復号する手段とを備え、
前記データ暗号化装置は、可搬性記憶媒体それぞれに固有な媒体固有情報を蓄積する媒体固有情報データベースと、共通鍵を蓄積する鍵データベースと、前記媒体固有情報データベースを検索して前記鍵データ要求に対応する媒体固有情報を求める手段と、前記鍵データベースを検索して前記鍵データ要求に対応する共通暗号鍵を求める手段と、前記媒体固有情報で前記共通暗号鍵を暗号化したものである前記鍵データを送信する手段とを備えた、暗号化システム。

【請求項５】　データを暗号化するデータ暗号化装置と、その暗号化されたデータを解読する暗号データ解読装置とから構成され、それらの間ではネットワークやバス等を介してデータの送受信が可能であり、
前記暗号データ解読装置は、それぞれに固有な媒体固有情報を有する可搬性記憶媒体を駆動する手段と、鍵データ要求を前記データ暗号化装置に送る手段と、前記データ暗号化装置から受信した鍵データを前記媒体固有情報の一部で復号する手段とを備え、
前記データ暗号化装置は、可搬性記憶媒体それぞれに固有な媒体固有情報を蓄積する媒体固有情報データベースと、共通鍵を蓄積する鍵データベースと、前記媒体固有情報データベースを検索して前記鍵データ要求に対応する媒体固有情報を求める手段と、前記鍵データベースを検索して前記鍵データ要求に対応する共通暗号鍵を求める手段と、前記媒体固有情報の一部で前記共通暗号鍵を暗号化してたものである前記鍵データを送信する手段とを備えた、暗号化システム。

【請求項６】　データを暗号化するデータ暗号化装置と、その暗号化されたデータを解読する暗号データ解読装置とから構成され、それらの間ではネットワークやバス等を介してデータの送受信が可能であり、
前記暗号データ解読装置は、それぞれに固有な媒体固有情報を有する可搬性記憶媒体を駆動する手段と、鍵データ要求を前記データ暗号化装置に送る手段と、前記データ暗号化装置から受信した鍵データを前記媒体固有情報の一部と本システムを利用するユーザを識別できるユーザ識別情報とを組み合わせたもので復号する手段とを備え、
前記データ暗号化装置は、可搬性記憶媒体それぞれに固有な媒体固有情報を蓄積する媒体固有情報データベースと、共通鍵を蓄積する鍵データベースと、前記媒体固有

情報データベースを検索して前記鍵データ要求に対応する媒体固有情報を求める手段と、前記鍵データベースを検索して前記鍵データ要求に対応する共通暗号鍵を求める手段と、前記媒体固有情報の一部とユーザ識別情報とを組み合わせたもので前記共通暗号鍵を暗号化したものである前記鍵データを送信する手段とを備えた、暗号化システム。

【請求項７】　データを暗号化するデータ暗号化装置と、その暗号化されたデータを解読する暗号データ解読装置とから構成され、それらの間ではネットワークやバス等を介してデータの送受信が可能であり、

前記暗号データ解読装置は、それぞれに固有な媒体固有情報を有する可搬性記憶媒体を駆動する手段と、データ要求を前記データ暗号化装置に送る手段と、前記データ暗号化装置から受信したデータを前記媒体固有情報に含まれる復号鍵を用いて復号する手段とを備え、

前記データ暗号化装置は、可搬性記憶媒体それぞれに固有な媒体固有情報を蓄積するデータベースと、前記データベースを検索して前記データ要求に対応する媒体固有情報内の復号鍵と一対をなす暗号鍵を得る手段と、前記暗号鍵を用いて前記要求されたデータを暗号化して送信する手段とを備えた、暗号化システム。

【請求項８】一対をなす復号鍵と暗号鍵とが、それぞれ公開鍵暗号方式における公開鍵と秘密鍵とであることを特徴とする請求項７に記載の暗号化システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号化された可搬性記憶媒体のデータを復号する暗号化システムに関し、特に、ＤＶＤ－ＲＯＭのＢＣＡ（Burst Cutting Area）内の暗号化情報を利用して、共通暗号鍵を配送する暗号化システムに関する。

【０００２】

【従来の技術】ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭなどのデータを不正なコピーから守るために、データの暗号化が行なわれている。暗号化されたデータを復元するための共通暗号鍵を安全に配布しなければ、暗号化した意味がなくなるので、共通暗号鍵の安全な配布方法が必要となる。共通暗号鍵の安全な配布方法の一つとして、公開鍵暗号方式を用いた方法が考えられる。図３は、公開鍵暗号方式を用いて共通暗号鍵を取得するために、従来の一般的な技術に従って想定したＤＶＤ－ＲＯＭ暗号化システムの構成図である。

【０００３】公開鍵暗号方式により共通暗号鍵を取得する方法を、図３を参照しながら説明する。前提条件として、ユーザＡがユーザＢから共通暗号鍵をオンラインで受け取るものとする。また、共通暗号鍵によって暗号化されたデータは、ユーザＡの手元（ＤＶＤ－ＲＯＭ）にあるものとし、必要な共通暗号鍵を指示可能なインデックス情報をユーザＡは指定できるものとする。共通暗号鍵の取得に際しては、本来以下の手順を必要とする。

【０００４】(1)ユーザＡからユーザＢに対して共通暗号鍵の取得依頼を行なう。

(1-1)取得対象の共通暗号鍵を指定するインデックス情報を得る。

(1-2)現在時刻などのランダムな情報を加えてリクエスト用の情報を作成する。

(1-3)ハッシュ関数を用いてリクエスト用の情報からハッシュ値を算出する。

(1-4)ユーザＡの秘密鍵をＩＣカード15から読み出す。

(1-4-1)秘密鍵を格納しているＩＣカード15に対してユーザＡにパスワードを入力させる。

(1-4-2)ＩＣカードリーダ14はパスワードが正しいかどうかを確認し、格納されている秘密鍵を読み出す。

(1-5)ユーザＡの秘密鍵を用いて、ハッシュ値に対して署名をほどこす。

(1-6)ユーザＡの公開鍵証明書をパソコンの記憶装置（ハードディスク）13等から得る。

(1-7)ユーザＢの公開鍵を証明書発行センター４などから得る。

(1-8)リクエスト用の情報と署名に対してユーザＢの公開鍵を用いてＲＳＡ暗号化を行ない、ユーザＡの公開鍵証明書とともにユーザＢに対して送信する。

【０００５】(2)ユーザＢがユーザＡからのリクエストの認証を行なう。

(2-1)ユーザＡの公開鍵証明書に対して、証明書発行センター４の公開鍵を用いて正当性を確認し、ユーザＡの公開鍵を得る。

(2-2)ユーザＢの秘密鍵をＩＣカード25から読み出す。

((1-4)と同様の手順)

(2-3)ユーザＢの秘密鍵を用いて、リクエスト用の情報と署名を復元する。

(2-4)ハッシュ関数を用いてリクエスト用の情報からハッシュ値を算出する。

(2-5)ユーザＡの署名に対して、ユーザＡの公開鍵を用いてハッシュ値を復元する。

(2-6)ステップ(2-4)と(2-5)で得たハッシュ値が同一であるかどうかを確認し、同一であればユーザＡからのリクエスト情報であることが確認できる。

【０００６】(3)ユーザＢはユーザＡに対して共通暗号鍵を送る。

(3-1)ユーザＢはリクエスト情報を用いて鍵ＤＢ22から必要な共通暗号鍵を特定する。

(3-2)現在時刻などのランダムな情報を加えて応答用の情報を作成する。

(3-3)ハッシュ関数を用いて応答用の情報からハッシュ値を算出する。

(3-4)ユーザＢの秘密鍵をＩＣカード25から読み出す。

((1-4)と同様の手順)

(3-5)ユーザＢの秘密鍵を用いて、ハッシュ値に対して

署名をほどこす。
(3-6)ユーザＢの公開鍵証明書をパソコンの記憶装置（ハードディスク）26等から得る。
(3-7)応答用の情報と署名に対してユーザＡの公開鍵を用いてＲＳＡ暗号化を行ない、ユーザＢの公開鍵証明書とともにユーザＡに対して送信する。
【０００７】(4)ユーザＡがユーザＢからの応答の認証を行ない、共通暗号鍵を得てデータを復元する。
(4-1)ユーザＢの公開鍵証明書に対して、証明書発行センター４の公開鍵を用いて正当性を確認し、ユーザＢの公開鍵を得る。
(4-2)ユーザＡの秘密鍵をＩＣカード15から読み出す。
((1-4)と同様の手順)
(4-3)ユーザＡの秘密鍵を用いて、応答用の情報と署名を復元する。
(4-4)ハッシュ関数を用いて応答用の情報からハッシュ値を算出する。
(4-5)ユーザＢの署名に対して、ユーザＢの公開鍵を用いてハッシュ値を復元する。
(4-6)ステップ(4-4)と(4-5)で得たハッシュ値が同一であるかどうかを確認し、同一であればユーザＢからの応答情報であることが確認できる。
(4-7)応答用の情報から共通暗号鍵を分離し、共通暗号鍵を得る。
(4-8)ＤＶＤ－ＲＯＭ12内の暗号化データから、共通暗号鍵によってデータを復元する。
【０００８】この方法によって各々の秘密鍵が守られる限り、通信路上での盗聴や他ユーザのなりすましといった攻撃に対しては、ほぼ完全に防御できる。また、共通暗号鍵を得た後、それをパソコンのハードディスクに直接格納せずに、ユーザＡの公開鍵で暗号化したままで格納しておくことで、格納時の攻撃にも耐えられる。
【０００９】
【発明が解決しようとする課題】しかし、この手順においては、証明書発行センターの公開鍵を用いて、お互いの公開鍵の正当性を認証しあう必要がある。また、それぞれの秘密鍵は一つしかないため、安全に保管するためには、上記のようにＩＣカードなどに格納してパスワードなどで管理を行なう必要があり、そのためには特別な装置（たとえばＩＣカードリーダ）が必要となる。このように、手順が複雑で、構成が大規模になるという問題がある。
【００１０】さらに、この手順におけるデータ盗聴という攻撃に対する安全性、なりすまし・改ざんという攻撃に対する安全性は個人の秘密鍵の管理の安全性に依存しているため、仕組みそのものは堅牢であっても、それぞれの個人の管理能力に全体の安全性が左右されるという点で、利用者が増加すればするほど、運用面での問題が大きくなる。
【００１１】本発明は、上記の問題を解決し、簡単な装置と手順でＤＶＤ－ＲＯＭ等の共通暗号鍵を安全に配布することを目的とする。
【００１２】
【課題を解決するための手段】本発明では、上記の課題を解決するために、暗号データ解読装置に、データ要求をデータ暗号化装置に送る手段と、データ暗号化装置から受信したデータを媒体固有情報で復号する手段とを設け、データ暗号化装置に、媒体固有情報データベースを検索してデータ要求に対応する媒体固有情報を求める手段と、媒体固有情報で送信データを暗号化して送信する手段とを設けた構成とする。このような構成とすることにより、配布済みの媒体固有情報を暗号鍵として、簡単な装置と手順でデータを暗号化して送ることができる。
【００１３】また、例えばＤＶＤ－ＲＯＭシステム等の端末装置に、受信したデータをＢＣＡデータで復号する手段を設け、センター装置に、ＢＣＡデータベースを検索してユーザのＢＣＡデータを求める手段と、ＢＣＡデータで送信データを暗号化して送信する手段とを設けた構成とする。このような構成とすることにより、配布済みのＤＶＤ－ＲＯＭのＢＣＡデータを暗号鍵として、簡単な装置と手順でデータを暗号化して送ることができる。
【００１４】また、データ暗号化装置（、例えばＤＶＤ－ＲＯＭシステム等のセンター装置）に、さらに、データ要求に応じてユーザデータベースを検索してユーザを認証する手段を設けた構成とする。このような構成とすることにより、簡単な装置と手順でユーザの認証ができる。
【００１５】また、暗号データ解読装置（、例えばＤＶＤ－ＲＯＭシステム等の端末装置）に、鍵データ要求をセンター装置に送る手段を設け、センター装置に、鍵データベースを検索して共通暗号鍵を求める手段と、ＢＣＡデータで共通暗号鍵を暗号化して送信する手段とを設けた構成とする。このような構成とすることにより、簡単な装置と手順で共通暗号鍵を暗号化して送ることができる。
【００１６】また、例えばＤＶＤ－ＲＯＭシステム等のセンター装置に、ＢＣＡデータの一部とユーザ識別情報（、例えば会員番号）を組み合わせたもので共通暗号鍵を暗号化して送信する手段を設け、端末装置に、受信した暗号化された共通暗号鍵をＢＣＡデータの一部と会員番号を組み合わせたもので復号する手段を設けた構成とする。このような構成とすることにより、簡単な装置と手順でよりいっそう安全に共通暗号鍵を暗号化して送ることができる。
【００１７】また、例えばＤＶＤ－ＲＯＭシステム等のセンター装置に、ＢＣＡデータに含まれる復号鍵と一対をなす暗号鍵を得る手段と、その暗号鍵で送信データを暗号化する手段を設け、端末装置に、復号鍵でその暗号化された送信データを復号する手段を設けた構成とす

る。また更には、この一対をなす復号鍵と暗号鍵とが、それぞれ公開鍵暗号方式における公開鍵と秘密鍵とである場合もあり、このような構成とすることにより、復号鍵から暗号鍵を計算することを実質上不可能とすることができるため、簡単な装置と手順でありながら、センター装置へのなりすまし・データの改ざんという攻撃を安易には行なえないようにした上で、安全にデータを暗号化して送ることができる。

【００１８】

【発明の実施の形態】本発明の請求項１に記載した発明は、データを暗号化するデータ暗号化装置と、その暗号化されたデータを解読する暗号データ解読装置とから構成され、それらの間ではネットワークやバス等を介してデータの送受信が可能であり、前記暗号データ解読装置は、それぞれに固有な媒体固有情報を有する可搬性記憶媒体を駆動する手段と、データ要求を前記データ暗号化装置に送る手段と、前記データ暗号化装置から受信したデータを前記媒体固有情報で復号する手段とを備え、前記データ暗号化装置は、可搬性記憶媒体それぞれに固有な媒体固有情報を蓄積するデータベースと、前記データベースを検索して前記データ要求に対応する媒体固有情報を求める手段と、要求されたデータを前記媒体固有情報で暗号化して送信する手段とを備えた暗号化システムであり、配布済みの媒体固有情報を暗号鍵とすることで、簡単な装置と手順でデータを暗号化して送ることができるという作用を有する。

【００１９】本発明の請求項２に記載した発明は、データを暗号化するセンター装置と、その暗号化されたデータを解読する端末装置とから構成され、それらの間ではネットワークやバス等を介してデータの送受信が可能であり、前記端末装置は、それぞれに固有な媒体固有情報であるＢＣＡデータを有するＤＶＤ－ＲＯＭを駆動する手段と、データ要求を前記センター装置に送る手段と、前記センター装置から受信したデータを前記ＢＣＡデータで復号する手段とを備え、前記センター装置は、ＤＶＤ－ＲＯＭそれぞれに固有なＢＣＡデータを蓄積するＢＣＡデータベースと、前記データベースを検索して前記データ要求に対応するＢＣＡデータを求める手段と、要求されたデータを前記ＢＣＡデータで暗号化して送信する手段とを備えた暗号化ＤＶＤ－ＲＯＭシステムであり、配布済みのＢＣＡデータを暗号鍵とすることで、簡単な装置と手順でデータを暗号化して送ることができるという作用を有する。

【００２０】本発明の請求項３に記載した発明は、データを暗号化するデータ暗号化装置と、その暗号化されたデータを解読する暗号データ解読装置とから構成され、それらの間ではネットワークやバス等を介してデータの送受信が可能であり、前記暗号データ解読装置は、それぞれに固有な媒体固有情報を有する可搬性記憶媒体を駆動する手段と、データ要求を前記データ暗号化装置に送る手段と、前記データ暗号化装置から受信したデータを前記媒体固有情報で復号する手段とを備え、前記データ暗号化装置は、可搬性記憶媒体それぞれに固有な媒体固有情報を蓄積する媒体固有情報データベースと、本システムを利用するユーザに関する情報を蓄積するユーザデータベースと、前記データ要求に応じて前記ユーザデータベースを検索して前記暗号データ解読装置のユーザを認証する手段と、前記媒体固有情報データベースを検索して前記データ要求に対応する媒体固有情報を求める手段と、要求されたデータを前記媒体固有情報で暗号化して送信する手段とを備えた暗号化システムであり、配布済みのＢＣＡデータを暗号鍵とすることで、簡単な装置と手順でユーザを認証してデータを暗号化して送ることができるという作用を有する。

【００２１】本発明の請求項４に記載した発明は、データを暗号化するデータ暗号化装置と、その暗号化されたデータを解読する暗号データ解読装置とから構成され、それらの間ではネットワークやバス等を介してデータの送受信が可能であり、前記暗号データ解読装置は、それぞれに固有な媒体固有情報を有する可搬性記憶媒体を駆動する手段と、鍵データ要求を前記データ暗号化装置に送る手段と、前記データ暗号化装置から受信した鍵データを前記媒体固有情報で復号する手段とを備え、前記データ暗号化装置は、可搬性記憶媒体それぞれに固有な媒体固有情報を蓄積する媒体固有情報データベースと、共通鍵を蓄積する鍵データベースと、前記媒体固有情報データベースを検索して前記鍵データ要求に対応する媒体固有情報を求める手段と、前記鍵データベースを検索して前記鍵データ要求に対応する共通暗号鍵を求める手段と、前記媒体固有情報で前記共通暗号鍵を暗号化したものである前記鍵データを送信する手段とを備えた暗号化システムであり、配布済みのＢＣＡデータを暗号鍵とすることで、簡単な装置と手順で共通暗号鍵を暗号化して送ることができるという作用を有する。

【００２２】本発明の請求項５に記載した発明は、データを暗号化するデータ暗号化装置と、その暗号化されたデータを解読する暗号データ解読装置とから構成され、それらの間ではネットワークやバス等を介してデータの送受信が可能であり、前記暗号データ解読装置は、それぞれに固有な媒体固有情報を有する可搬性記憶媒体を駆動する手段と、鍵データ要求を前記データ暗号化装置に送る手段と、前記データ暗号化装置から受信した鍵データを前記媒体固有情報の一部で復号する手段とを備え、前記データ暗号化装置は、可搬性記憶媒体それぞれに固有な媒体固有情報を蓄積する媒体固有情報データベースと、共通鍵を蓄積する鍵データベースと、前記媒体固有情報データベースを検索して前記鍵データ要求に対応する媒体固有情報を求める手段と、前記鍵データベースを検索して前記鍵データ要求に対応する共通暗号鍵を求める手段と、前記媒体固有情報の一部で前記共通暗号鍵を

暗号化したものである前記鍵データを送信する手段とを備えた暗号化システムであり、配布済みのＢＣＡデータの一部を暗号鍵とすることで、簡単な装置と手順で共通暗号鍵を暗号化して送ることができるという作用を有する。

【００２３】本発明の請求項６に記載した発明は、データを暗号化するデータ暗号化装置と、その暗号化されたデータを解読する暗号データ解読装置とから構成され、それらの間ではネットワークやバス等を介してデータの送受信が可能であり、前記暗号データ解読装置は、それぞれに固有な媒体固有情報を有する可搬性記憶媒体を駆動する手段と、鍵データ要求を前記データ暗号化装置に送る手段と、前記データ暗号化装置から受信した鍵データを前記媒体固有情報の一部と本システムを利用するユーザを識別できるユーザ識別情報とを組み合わせたもので復号する手段とを備え、前記データ暗号化装置は、可搬性記憶媒体それぞれに固有な媒体固有情報を蓄積する媒体固有情報データベースと、共通鍵を蓄積する鍵データベースと、前記媒体固有情報データベースを検索して前記鍵データ要求に対応する媒体固有情報を求める手段と、前記鍵データベースを検索して前記鍵データ要求に対応する共通暗号鍵を求める手段と、前記媒体固有情報の一部とユーザ識別情報とを組み合わせたもので前記共通暗号鍵を暗号化したものである前記鍵データを送信する手段とを備えた暗号化システムであり、配布済みのＢＣＡデータの一部と会員番号を組み合わせたものを暗号鍵とすることで、簡単な装置と手順で共通暗号鍵を暗号化して送ることができるという作用を有する。

【００２４】本発明の請求項７に記載した発明は、データを暗号化するデータ暗号化装置と、その暗号化されたデータを解読する暗号データ解読装置とから構成され、それらの間ではネットワークやバス等を介してデータの送受信が可能であり、前記暗号データ解読装置は、それぞれに固有な媒体固有情報を有する可搬性記憶媒体を駆動する手段と、データ要求を前記データ暗号化装置に送る手段と、前記データ暗号化装置から受信したデータを前記媒体固有情報に含まれる復号鍵を用いて復号する手段とを備え、前記データ暗号化装置は、可搬性記憶媒体それぞれに固有な媒体固有情報を蓄積するデータベースと、前記データベースを検索して前記データ要求に対応する媒体固有情報内の復号鍵と一対をなす暗号鍵を得る手段と、前記暗号鍵を用いて前記要求されたデータを暗号化して送信する手段とを備えた暗号化システムであり、送信データの暗号化と復号化に際して一対の関係にある互いに異なる鍵を用い、かつ、復号鍵は配布済みのＢＣＡデータに含まれているものを用いることで、簡単な装置と手順でありながら、センター装置へのなりすまし・データの改ざんという攻撃を安易には行なえないようにした上で、安全にデータを暗号化して送ることができるという作用を有する。

【００２５】本発明の請求項８に記載した発明は、請求項７に記載の発明において、一対をなす復号鍵と暗号鍵とが、それぞれ公開鍵暗号方式における公開鍵と秘密鍵とであることを特徴とする暗号化システムであり、送信データの暗号化と復号化に際して、公開鍵暗号方式における秘密鍵で暗号化を行ない、配布済みのＢＣＡデータに含まれている公開鍵で復号化を行なうようにすることで、復号鍵から暗号鍵を計算することを実質上不可能とできるため、簡単な装置と手順でありながら、センター装置へのなりすまし・データの改ざんという攻撃を排除した上で、安全にデータを暗号化して送ることができるという作用を有する。

【００２６】以下、本発明の実施の形態について、図面を参照しながら詳細に説明する。なお、本発明は以下の実施態様に何等限定されるものではなく、その要旨を逸脱しない範囲において、種々なる態様で実施し得る。

【００２７】本発明の実施の形態は、端末装置から共通暗号鍵要求をセンター装置に送り、センター装置では、ユーザのＢＣＡデータと共通暗号鍵を求め、ＢＣＡデータの一部と会員番号を組み合わせたもので共通暗号鍵を暗号化して返送し、端末装置では、受信した暗号化された共通暗号鍵をＢＣＡデータの一部と会員番号を組み合わせたもので復号する暗号化ＤＶＤ－ＲＯＭシステムである。

【００２８】図１は、本発明の実施の形態の暗号化ＤＶＤ－ＲＯＭシステムの構成を示す図である。図１において、端末装置１は、ユーザＡのパーソナルコンピュータである。ＤＶＤ－ＲＯＭドライブ11は、ＤＶＤ－ＲＯＭ12を読み出す装置である。ハードディスク装置13は、受信した共通暗号鍵などを格納しておく外部記憶装置である。センター装置２は、ユーザＢのパーソナルコンピュータである。ＢＣＡ－ＤＢ21は、すべてのＤＶＤ－ＲＯＭのＢＣＡデータを格納してあるデータベースである。鍵データベース22は、すべての共通暗号鍵を格納してあるデータベースである。ユーザＤＢ23は、会員番号（ユーザ識別情報）とパスワードの対応表と、会員番号とＢＣＡに含まれる情報（例えば後述のタイトル情報）の対応表等が格納されているデータベースである。ネットワーク３は、ユーザＡとユーザＢを結ぶ電話回線やインターネットなどの通信回線である。

【００２９】なお、ユーザＤＢに格納してある情報は、前記事項に何ら限定されるものではなく、本システムを利用する正規のユーザが正当に利用できる情報を管理しているものであればよく、例えば、そのユーザを特定・識別できる情報（ユーザ識別情報）とそのユーザに関する関する情報との対応表等が代表的である。もちろん、ユーザ識別情報だけでも一向に構わない。

【００３０】図２は、ＢＣＡ（Burst Cutting Area）の説明図である。ＢＣＡは、ＤＶＤ－ＲＯＭディスクの最内周のトラックに記録された12～188バイトのデータで

あり、ディスクごとに個別に、しかも改ざんできないように記録されるものである。ＢＣＡデータは、ＤＶＤのプレスにより記録されたデータと異なり、完成されたディスクの１枚ごとに、レーザ照射により書き込まれるものである。ＢＣＡについては、例えば、「ＤＶＤのＲＯＭディスクへの個別情報記録技術ＢＣＡ(BurstCutting Area)」(National Technical Report Vol.43,No.3 Jun.1997 pp.290-297.)に詳しく説明されている。

【００３１】図１のＤＶＤ－ＲＯＭシステムにおいて、共通暗号鍵を取得する手順を説明する。前提条件として、ユーザＡがユーザＢから、共通暗号鍵をオンラインで受け取るものとする。また、共通暗号鍵によって暗号化されたデータは、ユーザＡの手元（ＤＶＤ－ＲＯＭ）にあるものとし、必要な共通暗号鍵を指示可能なインデックス情報を、ユーザＡは指定できるものとする。

【００３２】ＢＣＡは、少なくとも以下の情報を持つ。

(a)タイトル情報：該当するＤＶＤ－ＲＯＭタイトルを特定する情報、

(b)個別識別情報：出版された同一タイトルの中での一枚毎を識別する情報、

(c)データ暗号化情報：取得データ（ここではユーザに配信するデータである共通暗号鍵）の暗号化に用いる情報。

【００３３】共通暗号鍵を取得する手順は、以下の通りである.

(1) ユーザＡからユーザＢに対して共通暗号鍵の取得依頼を行なう。

(1-1) ＤＶＤ－ＲＯＭドライブ11で、ＤＶＤ－ＲＯＭ12からＢＣＡを読み取り、取得対象の共通暗号鍵を指定するインデックス情報を、ＢＣＡ内のタイトル情報と個別識別情報とを用いて作成する。

(1-2) ユーザＡに対して会員番号・パスワードの入力を促す。あるいは、ハードディスクから会員番号・パスワードを読み込む。

(1-3) リクエスト用の情報としてインデックス情報、会員番号・パスワードの情報をユーザＢに対して送信する。

【００３４】(2) ユーザＢがユーザＡからのリクエストの認証を行なう。

(2-1) ユーザＡからのリクエスト用の情報から、会員番号・パスワードを抽出し、ユーザＤＢ23の会員番号とパスワードとの対応表からその正当性を確認する。

(2-2) ユーザＡからのリクエスト用の情報から、会員番号・タイトル情報・個別識別情報を抽出し、ユーザＤＢ23の会員番号とタイトル情報・個別識別情報との対応表から、ユーザＡがそのＤＶＤ－ＲＯＭを保持することを確認する。

【００３５】(3) ユーザＢはユーザＡに対して共通暗号鍵を送る。

(3-1) ユーザＢはリクエスト用の情報からインデックス情報を抽出し、鍵ＤＢ22から、必要な共通暗号鍵を特定する。

(3-2) インデックス情報中のタイトル情報・個別識別情報を用いて、ＢＣＡ－ＤＢ21のＢＣＡの一覧から、データ暗号化情報を取り出す。

(3-3) データ暗号化情報と会員番号とを用いて共通暗号鍵を暗号化し、ユーザＡに対して送信する。

【００３６】(4) ユーザＡがユーザＢの応答から共通暗号鍵を得てデータを復元する。

(4-1) ＢＣＡからデータ暗号化情報を抽出し、これと会員番号とを用いてユーザＢの応答を復元し、共通暗号鍵を抽出する。

(4-2) ＤＶＤ－ＲＯＭ12内の暗号化データから、共通暗号鍵によってデータを復元する。ただし、共通暗号鍵は会員番号とＢＣＡ内のデータ暗号化情報とで暗号化されたまま保存しておく。

【００３７】このシステムのメリットは、構成が簡単になること、安全性がある程度確保されるということである。また、送信するデータ（共通暗号鍵）の暗号化に用いる鍵が、既にユーザＡとユーザＢの両者にとって既知（＝ＢＣＡの一部を利用）であるので、鍵の交換をしなくてよいという利点がある。

【００３８】この鍵（ＢＣＡ内のデータ暗号化情報）はディスク一枚毎に異なるため、送信するデータ（共通暗号鍵）の解読には、ＤＶＤ－ＲＯＭ上のＢＣＡをも必要とするという点で、ある程度の安全性が確保される。手元に共通暗号鍵を格納する場合にも、ユーザＩＤ(会員番号)とＢＣＡ上の暗号化情報とを使って暗号化したままにしておけば、共通暗号鍵の安易なコピーを避けることができる。

【００３９】ここで、ユーザＩＤをも暗号化に用いるのは、仮にＢＣＡ上の暗号化情報のみを用いてデータ（共通暗号鍵）を暗号化した場合（この暗号化した結果を鍵情報と呼ぶものとする）には、ＤＶＤ－ＲＯＭと鍵情報とをセットで譲渡することでデータ（共通暗号鍵）を解読されてしまうからである。

【００４０】データ（共通暗号鍵）に対する対価が低い場合には、この程度の簡単な構成で多くのユーザに使用してもらえる環境を用意できる。特に、暗号化のためのコストが低いので、低価格のデータの配布に利用した場合にコスト的な負担が軽くて、安全性もかなり高く、取り扱いも容易であるという利点がある。

【００４１】このＤＶＤ－ＲＯＭシステムの弱点としては、会員番号とＢＣＡの双方を知られてしまった場合のような、強い攻撃には耐えられないということがある。しかし、通信路にはＢＣＡ全体を流さないので、ＢＣＡを知るためには、そのＤＶＤ－ＲＯＭを取得するか、ＢＣＡ－ＤＢから知る必要があるので、実用的には十分な強さがあるといえる。

【００４２】以上のように、本発明の実施の形態では、

ＤＶＤ－ＲＯＭシステムを、端末装置から共通暗号鍵要求をセンター装置に送り、センター装置では、ユーザのＢＣＡデータと共通暗号鍵を求め、ＢＣＡデータの一部と会員番号を組み合わせたもので共通暗号鍵を暗号化して返送し、端末装置では、受信した暗号化された共通暗号鍵をＢＣＡデータの一部と会員番号を組み合わせたもので復号するように構成したので、簡単な装置と手順で、ある程度の安全性を確保しつつ、共通暗号鍵を暗号化して送り、課金対象となるようなデータの取得と格納とが行なえる。

【００４３】また、このような構成を用いることの副次的な効果としては、ユーザＤＢにおいて、どのデータを販売済みかを管理しておくことにより、既に取得済みのデータを再取得する際には、課金を行なわないといった動作が可能となる。即ち、別のＰＣでＤＶＤ－ＲＯＭ上のデータを復号化するために再度共通暗号鍵を取得する場合には無料になるので、ＰＣを変えることに対する影響が少なくなる。

【００４４】なお、上記の手順の(3-2)(3-3)において、共通暗号鍵の暗号化に用いる情報として、公開鍵暗号方式における秘密鍵と会員番号とを用い、また、ＢＣＡの持つデータ暗号化情報として前記秘密鍵に対応する公開鍵を記録しておき、上記の手順の(4-1)において、ユーザＢの応答を復元する際に、前記公開鍵と会員番号とを用いる、いわゆる回復型署名を応用した構成とすることで、ユーザＡの管理下にある情報をどのように悪用しようとしても、送信データの暗号化をユーザＢ以外には行なえないようにすることができ、ユーザＢへのなりすましや送信データの改ざんといった攻撃を排除することが可能となる。これは、ユーザＡの管理下にある公開鍵はこれに対応する秘密鍵とは異なるものであり、また公開鍵からは秘密鍵を計算することは事実上不可能であるという、公開鍵暗号方式の性質によっている。

【００４５】なお、本実施の形態では、ネットワークで接続された端末装置とセンター端末とから構成されるシステムとして説明したが、キオスク端末のように端末装置とセンター端末とが一体型の装置で、バスで通信するような場合においても同様に適用できる技術であり、同様の効果が得られることは明らかである。

【００４６】なお、実施の形態ではＤＶＤ－ＲＯＭを例として説明したが、ＣＤ－ＲＯＭでもその他の可搬性記録媒体でも、媒体固有の情報を記録できるものであれば同様に適用できる技術であり、同様の効果が得られることは明らかである。

【００４７】

【発明の効果】本発明では、暗号データ解読装置（、例えばＤＶＤ－ＲＯＭシステムの端末装置）に、データ要求をデータ暗号化装置（、例えばＤＶＤ－ＲＯＭシステムのセンター装置）に送る手段と、受信したデータを媒体固有情報（、例えばＤＶＤ－ＲＯＭのＢＣＡデータ）で復号する手段とを設け、センター装置に、ＢＣＡデータベースを検索してユーザのＢＣＡデータを求める手段と、ＢＣＡデータで送信データを暗号化して送信する手段とを設けた構成としたので、配布済みのＢＣＡデータを暗号鍵として、簡単な装置と手順でデータを暗号化して送ることができるという効果が得られる。

【００４８】また、ＤＶＤ－ＲＯＭシステムのセンター装置に、さらに、データ要求に応じてユーザデータベースを検索してユーザを認証する手段を設けた構成としたので、簡単な装置と手順でユーザの認証ができるという効果が得られる。

【００４９】また、ＤＶＤ－ＲＯＭシステムの端末装置に、鍵データ要求をセンター装置に送る手段を設け、センター装置に、鍵データベースを検索して共通暗号鍵を求める手段と、ＢＣＡデータで共通暗号鍵を暗号化して送信する手段とを設けた構成としたので、簡単な装置と手順で共通暗号鍵を暗号化して送ることができるという効果が得られる。

【００５０】また、ＤＶＤ－ＲＯＭシステムのセンター装置に、ＢＣＡデータの一部とユーザを一意に識別できるユーザ識別情報（、例えば会員番号）を組み合わせたもので共通暗号鍵を暗号化して送信する手段を設け、端末装置に、受信した暗号化された共通暗号鍵をＢＣＡデータの一部と会員番号を組み合わせたもので復号する手段を設けた構成としたので、簡単な装置と手順でより安全に共通暗号鍵を暗号化して送ることができるという効果が得られる。

【００５１】また、ＤＶＤ－ＲＯＭシステム等のセンター装置に、ＢＣＡデータに含まれる復号鍵と一対をなす暗号鍵を得る手段と、その暗号鍵で送信データを暗号化する手段を設け、端末装置に、復号鍵でその暗号化された送信データを復号する手段を設けた構成とする。また更には、この一対をなす復号鍵と暗号鍵とが、それぞれ公開鍵暗号方式における公開鍵と秘密鍵とである場合もあり、このような構成とすることにより、復号鍵から暗号鍵を計算することを不可能にできるため、簡単な装置と手順でありながら、センター装置へのなりすまし・データの改ざんという攻撃を安易には行なえないようにした上で、安全にデータを暗号化して送ることができるという効果が得られる。

【図面の簡単な説明】

【図１】本発明の実施の形態の暗号化ＤＶＤ－ＲＯＭシステムの構成図、

【図２】ＤＶＤ－ＲＯＭのＢＣＡの説明図、

【図３】公開鍵暗号を用いたＤＶＤ－ＲＯＭシステムの構成図である。

【符号の説明】

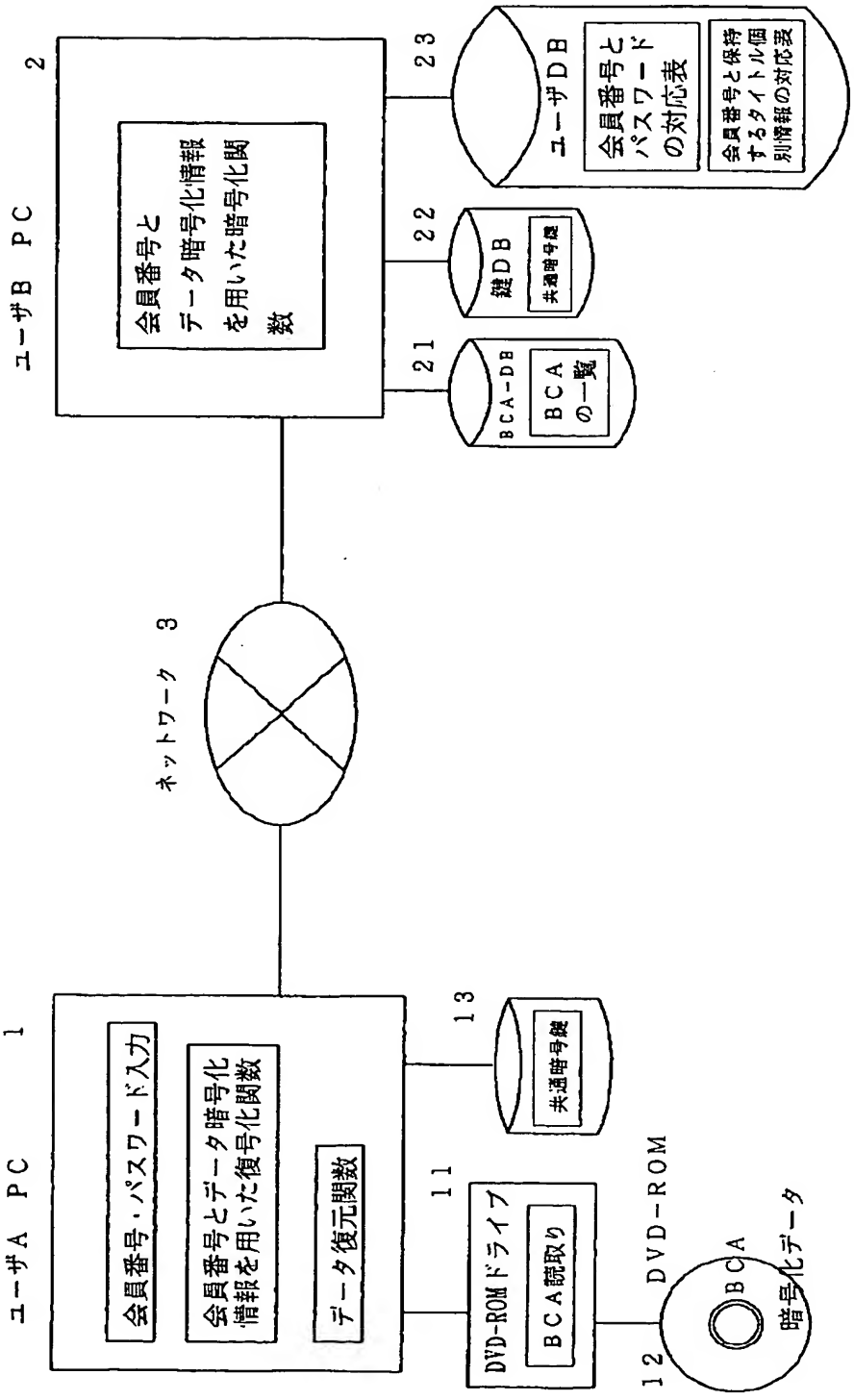
１　端末装置

２　センター装置

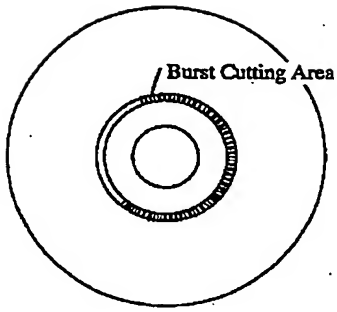
３　ネットワーク

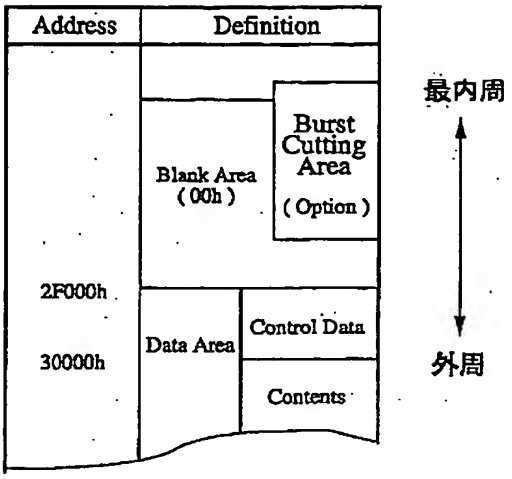
4　公開鍵証明書発行センター
11　DVD－ROMドライブ
12　DVD－ROM
13、26　ハードディスク
14、24　ICカードリーダー
15、25　ICカード
21　BCAデータベース
22　鍵データベース
23　ユーザデータベース

【図1】

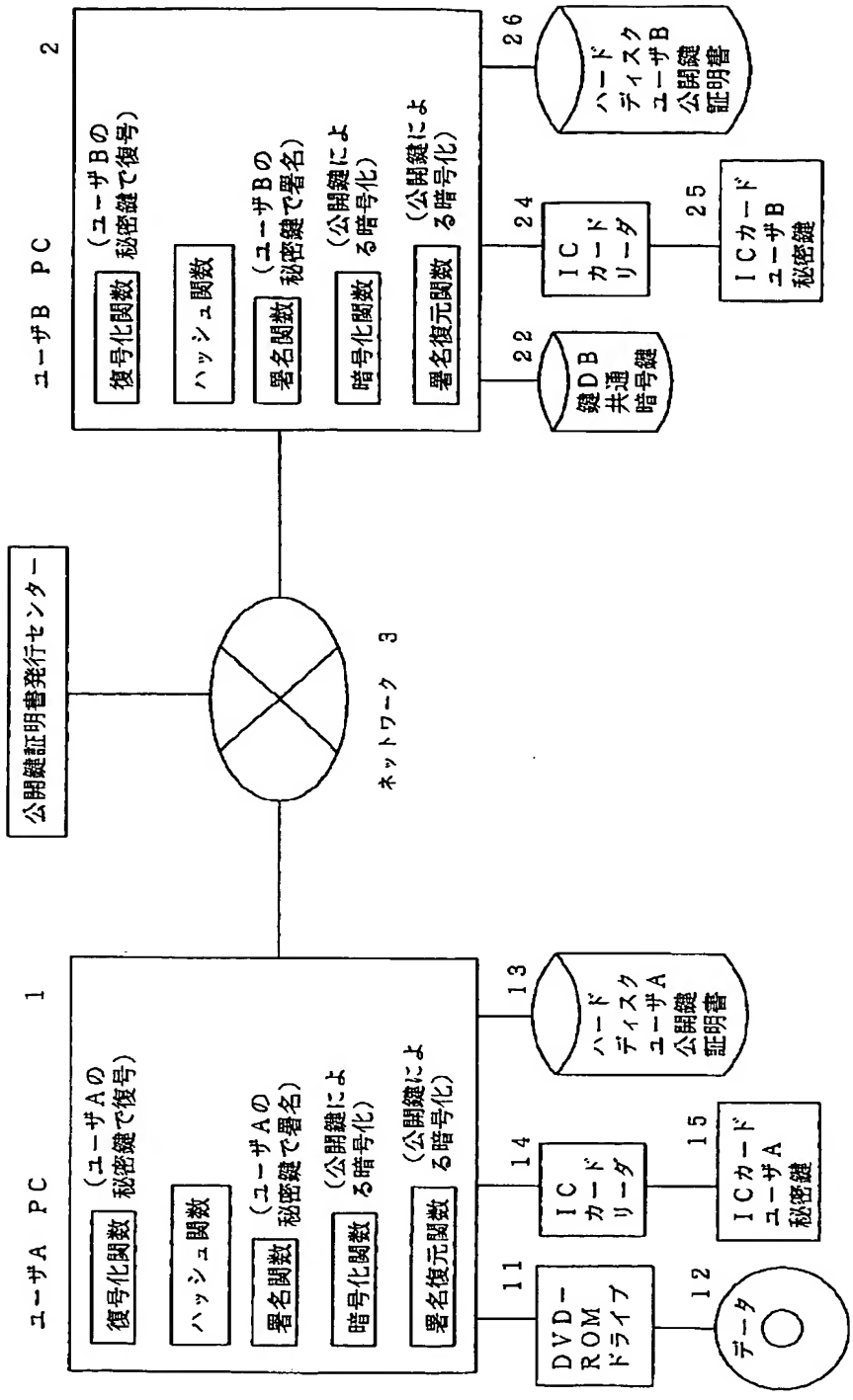


【図２】


Burst Cutting Area


Address
Definition
Blank Area
(00h)
Burst
Cutting
Area
(Option)
2F000h
Data Area
Control Data
30000h
Contents
最内周
外周

【図３】



フロントページの続き

(51) Int.Cl.[6]	識別記号	FI
		H04L 9/00　601Z